Cryptacus Newsletter

April'17 Cryptacus Newsletter

Welcome to the latest edition of the monthly Cryptacus.eu newsletter, offering a glimpse into recent developments in the IoT cryptanalysis area. We'd love to receive more of your contributions, comments & feedback at cryptacus.newsletter@irisa.fr

News from the Chair

by Gildas Avoine

Dear Cryptacus Members,

April 30^{th} is the end of the current yearly grant period. During this period, Cryptacus organized a meeting at Sophia-Antipolis in France, and a recent workshop at Sutomore in Montenegro. It was a great success and an enjoyable experience, in a big part due to the excellent organisation my Milena Djukanovic, and it even got some coverage by Montenegro's Ministry of Research (see `https://goo.gl/ug1GpF`).

We also funded 6 grants for short-term scientific missions from, or to, the following countries: Belgium, Finland, Greece, Italy, Israel, Netherlands, Spain, Sweden, and Switzerland. Cryptacus also funded the 14 speakers who participated in the recent Montenegro's workshop. They came from Finland, France, Greece, Italy, Luxembourg, Serbia, Turkey, and the United Kingdom.

Another workshop will likely be organized in Fall 2017, and a training school in Spring 2018. More information will be provided in the next newsletter.

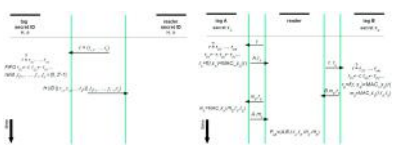
In the meanwhile, Cryptacus' members are invited to collaborate on their own. Several initiatives have also been launched: a H2020 project proposal (see the email sent by Billy Brumley), a collaborative book about cryptanalysis in ubiquitous computing systems (Julio Hernandez-Castro will provide us with more details in the coming weeks), and also do not forget to promote STSMs, open faculty positions, and PhD theses in the newsletter.

In addition, Cryptacus is looking for a volunteer to manage the website. Pascal Junod has been the website manager for two years but he got a new position and he decided to resign from Cryptacus.
Pascal did a great job during two years to set up and manage the website.
Cryptacus is consequently now looking for a volunteer to replace Pascal. Now that the website site is launched, the task is pretty lightweight. Pascal said he will ensure the transition. Please contact me if you want to volunteer.

All the best.

Gildas

Recommended reading



This month we will start with a paper on Grouping Proofs by Denis

Trček. It was published in the Journal Sensors in 2016, number 16, volume 1. Its title is *Wireless Sensors Grouping Proofs for Medical Care and Ambient Assisted-Living Deployment*, and you can read it at `http://www.mdpi.com/1424-8220/16/1/33`.

The paper provides a lengthy and detailed review of the grouping proofs literature, detailing the many security issues encountered and tries to extract lessons and prudent engineering practices from them. It offers a new lightweight grouping proof with privacy provisioning, and with a formal security proof in HLPSL for AVISPA.

Funding News

Following our H2020 Opportunities presentation in Montenegro, we are happy that both Miodrag Mihaljevic and Billy Brumley gave it a try to mount consortia and proposals for the Crypto call. Good luck to both and thanks for moving things forward! I am sure that many great things will come in the future when we target other calls with more time. This is why we will continue to arrange another H2020 session on the next Cryptacus meeting. It will be a good opportunity to discuss some of the most relevant future calls in detail, and plan well ahead of them to increase your success chances.
If you are interested in participating in this session, and particularly if you want to briefly present a project idea to get feedback and potentially start building-up a consortium, please contact me for booking a slot.

Open Positions

Please send us any employment opportunity you want to publicize in the newsletter.

There are plenty of interesting open positions, such as:

- A PhD Scholarship is open for a thesis on forensics in embedded systems in the research group of Prof. Gildas Avoine in Rennes (France). The PhD thesis will start in Fall 2017. Applications must be sent before April 20^{th}, 2017. More information at `http://www.avoine.net/forensics_avoine.pdf`
- Prof. Milutinovic wants us to announce this position with Maxeler CyberSecurity `https://www.maxeler.com/about-us/careers/opportunities/#cyber_sec`
- Professor in Cryptology at Aalto University. Deadline is the 01/04/2017. More info at `https://goo.gl/7hy5GL`
- Professorship in Computer Networks and Communication Systems at Brandenburg University of Technology (BTU). They mention their interest in the areas of "the internet of things" and "security in computer networks". The application deadline is the 06/04/2017. German and English fluency required. More info at `https://www.b-tu.de/fakultaet1/`.

  In addition, a good number of positions in the other side of the channel have recently opened or are about to close:
- Lecturer in Information Security at the Information Security Group of Royal Holloway, University of London. Deadline is the 9^{th} of April, and the salary £41,458 to £49,059 per annum. Needless to say, this is the largest information security group in the UK, and one of the most prestigious. More info at `https://goo.gl/0YZzp2`. They also offer `https://goo.gl/hWCgvY` a more teaching-focused position at the same Lecturer level.
- Lecturer in Computer Security at the School of Computer Science, within the College of Engineering and Physical Sciences of the University of Birmingham. Deadline for applications is the 2^{nd} of April. Salary range is £39,324 to £52,793, for a full time, permanent position. Birmingham has a much smaller security group but they have some very talented people and have recently recruited very well and continue to attract talent. Also one of the very top security groups in the UK. For applying, check `https://goo.gl/yDLQS9`.

For other interesting positions all across Europe, please check the recently revamped "Researchers in Motion" portal `https://euraxess.ec.europa.eu/`.

Proposals for STSMs

EURECOM
Sophia Antipolis

By now, you should be already familiar with what Short Term Scientific Missions (or STSMs, for short) are, but we have a healthy budget for them within the Cryptacus project and not enough demand.

Until somebody sends more proposals, we will repeat the STSM offers of the past, including that of Aurélien Francillon and mine.

- "At Eurecom we are actively working on analyzing embedded devices software and

building methodologies and tools for this. An example of that is ourvopen source Avatar Framework (see `http://s3.eurecom.fr/tools/avatar/`) which is aimed to reverse engineer devices and search for vulnerabilities. We are happy to receive visitors interested in the topic, for example to get help to start using the Avatar framework on a given device."

- I will be happy to receive anyone interested in investigating the many limitations and pitfalls of the PRNGs and the TRNGs currently in use on IoT devices.

Blogs and posts to read

This month, we can recommend a short piece on PKI for IoT by Jeremy Rowley on Issue 53 of the Insecure Magazine by HelpNetSecurity.com at `https://www.helpnetsecurity.com/insecuremag/issue-53-march-2017/`

Another interesting news item is the development of a new Metasploit extension for testing the security of IoT devices. This extension is called RFTransceiver and will let us detect and scan wireless devices operating outside the 802.11 spec. This could be very useful for pentesters and researchers finding vulnerabilities, for example, in smart lighting systems using the Zigbee communication protocol, network-enabled alarms, surveillance and door control systems, etc. More info at `https://goo.gl/RuXDEV`. This is an useful addition to their IoTseeker free tool for finding connected IoT devices and checking for default passwords, that can be downloaded from `https://information.rapid7.com/iotseeker`.

Event calendar

The first spring school (thanks Stefan!) on security and correctness in IoT, takes place May 8-12 in Graz, Austria. Topics range from software exploits and hardware side-channels to formal methods for security verification. Standard registration is open until April 16. More info at `http://springschool.iaik.tugraz.at/`.

The program is very interesting, and brings in some of the best in the area (including many Cryptacus people) and lots of practical labs. In addition, they offer a limited number of student stipends to cover registration.

The summer school on real-world crypto and privacy organised by Lejla will take place in Sibenik (Croatia), June 5 to 9. Highly recommended, for all ages! Registration will open early February 2017. More relevant info at `https://goo.gl/cSCcUZ`.

ESORICS is this year in beautiful Oslo, from 11-15 September. Submission deadline is April 19^{th}. Hope to see many of you there!

Indocrypt is this year in Chennai, with a paper submission deadline of August 20^{th} and notification on the 5^{th} of October. The conference will be from 10-13 December.

Agusti Solanas is organising a special session in a IEEE Conference on Smart Health with many topics of interest for Cryptacus members, including: Security, privacy and trust management for Smart Healthcare services/applications, Lightweight cryptography for Smart Healthcare devices and systems and Cryptanalysis of protocols for Smart Healthcare devices. More info at `http://rtsi2017.ieeesezioneitalia.it/tech_sessSH.html`

See you all very soon!

Best,
Julio Hernandez-Castro